UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,265	12/28/2001	Koichi Ito	1573.1010	2775

21171 7590 10/19/2005

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER
SZYMANSKI, THOMAS M

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 10/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/028,265	Applicant(s) ITO ET AL.	
	Examiner Thomas Szymanski	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 August 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) *10-15,22-24,26 and 28* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,16-21,25 and 27* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *8/12/03, 2/1/02*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-9, 16-21, 25, and 27 are drawn to an encryption device and an encryption program wherein mask values or masked fixed tables are selected depending upon a randomly generated number, classified in class 380, subclass 263.

II. Claims 10-15, 22-24, 26, and 28 are drawn to an encryption device and an encryption program wherein an encryption process is selected from a plurality of available processes depending on a generated random number, classified in class 380, subclass 46.

The inventions are distinct, each from the other because of the following reasons:

2. Inventions I and II are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination as claimed because the device of group II has separate utility by randomly selecting a given encryption process. The subcombination has separate utility such as encrypting via randomly selecting a mask or mask fixed table.

3. Because these inventions are distinct for the reasons given above and the search required for Group I is not required for Group II, restriction for examination purposes as indicated is proper.

4. Claims 10-15, 22-24, 26, and 28 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected invention, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on 8/10/2005.

5. Claims 1-9, 16-21, 25, and 27 have been examined.

Specification

6. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

7. The applicant is requested to review the specification and update the status of all co-pending applications made mention of, replacing attorney docket numbers with current U.S. application or patent numbers when appropriate. References to U.S. applications or patents should make it clear as to what the number refers (e.g. U.S. Patent No. #), instead of listing only the number.

Claim Rejections - 35 USC § 101

8. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

9. Claims 1-9, and 16-21 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. As stated the claims refer to material that is not tangible in nature but merely a formulation. In order for such claimed subject matter to be statutory it must be contained within a computer readable medium or relate to being conceived within a tangible medium of some other regard.

Claim Rejections - 35 USC § 112

10. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claims 6 and 8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

12. The applicant has claimed the following equation "($C_{0,j}$ XOR $C_{1,j}$) V....V ($C_{q-2,j}$ XOR $C_{q-2,j}$) = $(11111111)_2$". The claimed equation is inconsistent with the specification, as provided therein the equation is "($C_{0,j}$ XOR $C_{1,j}$) V....V ($C_{q-2,j}$ XOR $C_{q-1,j}$) = $(11111111)_2$". For the purpose of clarity within further examination the examiner has taken the equation as stated within the specification to be that which is appropriate.

13. Equation (16) within the specification is defined as "($d_{0,j}$ XOR $d_{1,j}$) V....V ($d_{q-2,j}$ XOR $d_{q-1,j}$) = $(11111111)_2$" within the claims the applicant has claimed the following

equation “$(d_{0,j}$ XOR $d_{1,j})$ V....V $(d_{q-2,j}$ XOR $d_{q-2,j}) = (11111111)_2$” this second equation provides for a final determination that will always equal 0. Therefore, for purposes of further examination the examiner has taken the equation as provided within the specification to be the correct occurrence.

Claim Rejections - 35 USC § 102

14. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

15. Claims 1-9, 16-21, 25, and 27 as best understood are rejected under 35 U.S.C. 102(b) as being anticipated by Kawamura et al European Patent Application EP 0981223 A2.

16. Regarding Claim 1: q fixed values, where q is an integer (paragraph 0010) The art refers to a value (i) that is a positive integer.

A selector for selecting one of q said fixed values in response to a randomly generated number (paragraph 0009, 0043-0044)

XORing an input with an XOR of a key with said selected fixed value (Fig 2, Fig 4, paragraph 0026-0029) As stated the input values are XORed with the randomly selected pattern.

17. Regarding Claims 2 and 4: q sets of masked fixed tables (paragraph 0010, Fig 4, 9) As stated previously there are (i) sets of tables for the masks.

Second selector for selecting one of q sets of masked fixed tables in response to a random number. Nonlinear transforming an input in accordance with the selected set of fixed tables (Fig 4, paragraph 0026-0030) The transform takes place as a function of the inverse of p. This provides for the stated nonlinear transformation.

18. Regarding Claim 3: encrypting unit comprising first XOR and nonlinear transform means (Fig 1, 2, 4, paragraph 0009, 0022, 0029)

Second XOR means for XORing an input to the encryption unit with a fixed value selected in response to the random number (Fig 4)

Third XOR means for XORing an output of the encryption unit with the fixed value selected in response to the random number (Fig 4) The system as denoted within figure 4 provides for a means of XORing the input, and output, as well as performing the nonlinear transform as described previously all within the scope of XORing the necessary values to obtain the intermediate masked values.

19. Regarding Claims 5 and 18: Plurality of encrypting rounds (Fig 1, paragraph 0019-0024)

Fixed tables for the plurality of respective rounds are identical (Fig 1, Fig 4) As shown once a random value indicates the table for performing that particular mask function it does not change over the permutations.

20. Regarding Claim 6: "($C_{0,j}$ XOR $C_{1,j}$) V....V ($C_{q-2,\,j}$ XOR $C_{q-1,j}$) = $(11111111)_2$", is satisfied, where a fixed table before masking is defined as S[x], and j-th masked table is defined as S_j[x XOR $C_{i,j}$] XOR $d_{i,j}$ (j = 0, 1, ...15) (Fig 1, Fig 4, Fig 8, Fig 10) As shown

per the iterations j is a value of 16 as shown. Additionally, the values are reiterated per the implementation until such a value is reached.

21. Regarding Claim 7: The number of sets of tables is q=2, and $C_{0,j}$ Xor $C_{1,j}$ = $(10101010)_2$ or $(01010101)_2$, is satisfied, where a fixed table before masking is defined as S[x], and j-th masked table is defined as S_j[x XOR $C_{i,j}$] XOR $d_{i,j}$ (j = 0, 1, ...15) (Fig 1, 4, 10, paragraph 0026-0029, 0055) As shown within the figure there are exactly two separate possibilities for tables.

22. Regarding Claim 8: "($d_{0,j}$ XOR $d_{1,j}$) V....V ($d_{q-2,j}$ XOR $d_{q-1,j}$) = $(11111111)_2$", is satisfied, where a fixed table before masking is defined as S[x], and j-th masked table is defined as S_j[x XOR $C_{i,j}$] XOR $d_{i,j}$ (j = 0, 1, ...15) (Fig 1, Fig 4, Fig 8, Fig 10) As shown per the iterations j is a value of 16 as shown. Additionally, the values are reiterated per the implementation until such a value is reached. The structure of the system as provided within the diagram provides for such a conclusion.

23. Regarding Claim 9: Nonlinear transform means being sub-byte means (Fig 4, paragraph 0027-0029) As shown the operations performed are done so in a bitwise manner, as such providing for a sub-byte means of transformation.

Encryption device comprising means for shifting an input, and mixed-columning an input (Figs 1-8, paragraph 0027-0030) As per the implementation of the Kawamura system in order to transform and perform the necessary operations the device contains such means.

24. Regarding Claim 16: each of a plurality of encrypting rounds comprises nonlinear transform means for nonlinearly transforming an input thereto, and XOR

means for XORing a first input thereto with a second input thereto (Fig 1-2, paragraph 0019-0023) Each iteration provides for the necessary components.

25. Regarding Claim 17: nonlinear transform means comprises a plurality of nonlinear transform means and a selector for selecting one of said plurality of nonlinear transform means (Fig 1, 2, 4, 10 paragraph 0019-0020, 0028) Kawamura sets forth the method by which the particular set of nonlinear transform means is selected and each having a plurality therein.

26. Regarding Claim 19: a mask is cancelled over subsequent ones of the rounds (Fig 19-22) As is the purpose of the invention the mask must be cancelled or removed before the value can be passed on and used for its originally intended purpose.

27. Regarding Claim 20: masking is performed in each of a second plurality of encrypting rounds of said first plurality of encrypting rounds, said second plurality being smaller that the first plurality (Fig 1, paragraph 0020) As stated the successive rounds of the permutation occur on subsets of the data and are therefore smaller.

28. Claims 21, 25, and 27 are merely recitations of claims 1-9, and 16-20 in the form of a computer program and as such are rejected on the same basis.

Conclusion

29. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Applicant is reminded that in amending in response to a rejection of claims, the patentable novelty must be clearly shown in view of the state of art

disclosed by the references cited and the objections made. Applicant must show how the amendments avoid such references and objections. See 37 CFR 1.111(c).

30. Inquiries concerning this communication or earlier communications from the examiner should be directed to Thomas M. Szymanski who can be reached at (571) 272-8574. The examiner's normal working schedule is between the hours 8:00am – 4:30pm (EST), Monday – Friday.

31. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

32. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JL

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100